

SIEMS Week 1 Homework



Introduction

This assignment is to demonstrate the core concepts of the Splunk software.

Step #1 : The Need For Speed

We are tasked with creating a search field in which we can see the effect a recent DDoS attack has had on the upload and download speeds at the Vandalay corporation.

Additionally we are requested to make a table in the report to show findings.

The screenshot shows the Splunk 8.2.4 interface. The search bar contains the command: `source="server_speedtest.csv" host="65dc0e77793d" sourcetype="csv" | eval ratio = 'UPLOAD_MEGABITS' / 'DOWNLOAD_MEGABITS' | table _time,IP_ADDRESS,UPLOAD_MEGABITS ,DOWNLOAD_MEGABITS,ratio`. The results table displays 23 events from February 22, 2020, at 7:21:56 AM. The columns are: _time, IP_ADDRESS, UPLOAD_MEGABITS, DOWNLOAD_MEGABITS, and ratio. The data shows varying upload and download speeds across different IP addresses, with a notable peak in upload speed around 2020-02-24 18:30:00.

_time	IP_ADDRESS	UPLOAD_MEGABITS	DOWNLOAD_MEGABITS	ratio
2020-02-24 20:30:00	198.153.194.2	26.51	126.91	0.2089
2020-02-24 18:30:00	198.153.194.2	25.51	125.91	0.2026
2020-02-24 16:30:00	198.153.194.1	24.51	124.91	0.1962
2020-02-23 23:30:00	198.153.194.2	8.51	123.91	0.0687
2020-02-23 23:30:00	198.153.194.1	7.51	122.91	0.0611
2020-02-23 22:30:00	198.153.194.1	6.51	78.34	0.0831
2020-02-23 20:30:00	198.153.194.2	4.23	65.34	0.0647
2020-02-23 18:30:00	198.153.194.2	3.43	17.56	0.195
2020-02-23 14:30:00	198.153.194.1	1.83	7.87	0.233
2020-02-23 14:30:00	198.153.194.2	2.19	12.76	0.172
2020-02-22 23:30:00	198.153.194.2	9.51	109.16	0.0871
2020-02-22 22:30:00	198.153.194.2	8.51	109.91	0.0774
2020-02-22 20:30:00	198.153.194.2	7.51	108.91	0.0690

- 1.Based on the report, the attack happened on 2-23-2020 at 14:30.
2. The systems took approximately 9 hours to recover to baseline.

Step #2 : Are We Vulnerable

We are tasked with finding the critical vulnerabilities on the database then creating an alert to monitor for future critical events. This is shown in the screenshots below.

Thu 16:48

Search | Splunk 8.2.4 - Mozilla Firefox

localhost:8000/en-US/app/search/search?earliest=0&latest=&q=search source%3Dnessus_logs..

Administrator Messages Settings Activity Help Find

New Search

source="nessus_logs.csv" host="65dc0e77793d" sourcetype="csv" severity="critical" dest_ip="10.11.36.23"

49 events (before 2/3/22 9:48:16.000 PM) No Event Sampling

Events (49) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out + Zoom to Selection Deselect

1 hour per column

List Format 20 Per Page ▾

Selected Fields: host 1, severity 1, source 1, sourcetype 1

Interesting Fields: # bid 15, # cvss 22, # cvss_base_score 3, # cvss_vector 3, # date_hour 13, # date_mday 2, # date_minute 35, # date_month 1, # date_second 31, # date_wday 2, # date_year 1, # date_zone 1, # dest 1

Time: 2/20/20 5:33:01.000 PM

Event

```

> 2/20/20 5:33:01.000 PM
    "start_time": "Thu Feb 20 17:33:01 2020", "end_time": "Thu Feb 20 17:33:01 2020", "dest_dns": "HOST-003", "dest_nt_host": "ops-sys-006", "dest_mac": "ad:7b:3d:db:49:8b", "dest_ip": "10.11.36.13", "os": "Cisco Router", "dest_port_proto": "el-random(827/tcp)", "severity_id": "4", "signature_id": "12258", "signature_name": "Additional DNS H ostnames", "splunk_ta-nessus-end-of-event": "2029-02-20T18:03:12.000+0000", "host": "65dc0e77793d", "severity": "critical", "source": "nessus_logs.csv", "sourcetype": "csv"}, {"start_time": "Thu Feb 20 17:33:01 2020", "end_time": "Thu Feb 20 17:33:01 2020", "dest_dns": "HOST-003", "dest_nt_host": "ops-sys-006", "dest_mac": "ad:7b:3d:db:49:8b", "dest_ip": "10.11.36.23", "os": "Cisco Router", "dest_port_proto": "el-random(827/tcp)", "severity_id": "4", "signature_id": "12258", "signature_name": "Additional DNS Hostnames", "splunk_ta-nessus-end-of-event": "2029-02-20T17:39:19.000+0000", "host": "65dc0e77793d", "severity": "critical", "source": "nessus_logs.csv", "sourcetype": "csv"}, {"start_time": "Thu Feb 20 17:27:48 2020", "end_time": "Thu Feb 20 17:27:48 2020", "dest_dns": "HOST-003", "dest_nt_host": "ops-sys-006", "dest_mac": "0b:4a:fe:06:36:92", "dest_ip": "10.11.36.29", "os": "Microsoft Windows XP Service Pack 3", "dest_port_proto": "general", "severity_id": "4", "signature_id": "12122", "signature_name": "Terminal Services Encryption Level is not FIPS-140 Compliant", "splunk_ta-nessus-end-of-event": "2020-02-20T17:39:19.000+0000", "host": "65dc0e77793d", "severity": "critical", "source": "nessus_logs.csv", "sourcetype": "csv"}, {"start_time": "Thu Feb 20 17:27:48 2020", "end_time": "Thu Feb 20 17:27:48 2020", "dest_dns": "HOST-003", "dest_nt_host": "ops-sys-006", "dest_mac": "0b:4a:fe:06:36:92", "dest_ip": "10.11.36.23", "os": "Microsoft Windows XP Service Pack 3", "dest_port_proto": "general", "severity_id": "4", "signature_id": "12122", "signature_name": "Terminal Services Encryption Level is not FIPS-140 Compliant", "splunk_ta-nessus-end-of-event": "2020-02-20T17:39:19.000+0000", "host": "65dc0e77793d", "severity": "critical", "source": "nessus_logs.csv", "sourcetype": "csv"}, {"start_time": "Thu Feb 20 17:27:48 2020", "end_time": "Thu Feb 20 17:27:48 2020", "dest_dns": "HOST-003", "dest_nt_host": "ops-sys-006", "dest_mac": "0b:4a:fe:06:36:92", "dest_ip": "10.11.36.23", "os": "Microsoft Windows XP Service Pack 2", "dest_port_proto": "general", "severity_id": "4", "signature_id": "12122", "signature_name": "Terminal Services Encryption Level is not FIPS-140 Compliant", "splunk_ta-nessus-end-of-event": "2020-02-20T17:39:19.000+0000", "host": "65dc0e77793d", "severity": "critical", "source": "nessus_logs.csv", "sourcetype": "csv"}, {"start_time": "Thu Feb 20 17:27:48 2020", "end_time": "Thu Feb 20 17:27:48 2020", "dest_dns": "HOST-003", "dest_nt_host": "ops-sys-006", "dest_mac": "0b:4a:fe:06:36:92", "dest_ip": "10.11.36.23", "os": "Microsoft Windows XP Service Pack 2", "dest_port_proto": "general", "severity_id": "4", "signature_id": "12122", "signature_name": "Terminal Services Encryption Level is not FIPS-140 Compliant", "splunk_ta-nessus-end-of-event": "2020-02-20T17:39:19.000+0000", "host": "65dc0e77793d", "severity": "critical", "source": "nessus_logs.csv", "sourcetype": "csv"}]
```

Thu 23:02

Severity "Critical" Notification | Splunk 8.2.4 - Mozilla Firefox

localhost:8000/en-US/app/search/alert?s=%2FservicesNS%2Fnobody%2Fsearch..

Administrator Messages Settings Activity Help Find

Severity "Critical" Notification

This alert is designed to alert when a critical event has happened. This alert will update every critical event that happens in order to address it.

Enabled: Yes. Disable

App: search

Permissions: Shared in App. Owned by admin. Edit

Modified: Feb 3, 2022 9:47:40 PM

Alert Type: Scheduled. Daily, at 6:00. Edit

Trigger Condition: Number of Results is > 0. Edit

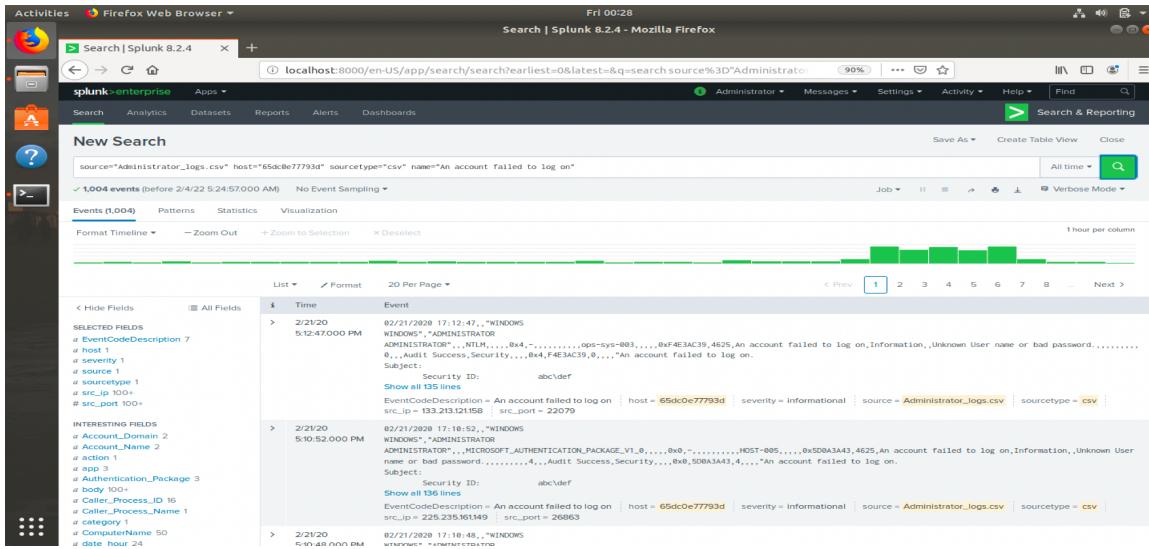
Actions: 1 Action Edit

Send email

There are no fired events for this alert.

Step #3: Drawing the (base)line

We are tasked with monitoring the Admin logs for failed login attempts. We are then required to figure out what a baseline is for the Admin and create an alert to trigger when that threshold has been exceeded.



Based on the report shown the attack began at 0800 on 2/21/2020 and continued until 1400. The entire attack was 6 hours until the baseline returned.

The baseline for the failed logins was estimated at 20 attempts an hour with 30 being the threshold set for the alert.

The alert created can be viewed below:

